

FORM PTO-1390 (Modified)
(REV 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

TRANSMITTAL LETTER TO THE UNITED STATES

T2146-907343

DESIGNATED/ELECTED OFFICE (DO/EO/US)

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR

CONCERNING A FILING UNDER 35 U.S.C. 371

09/869435

INTERNATIONAL APPLICATION NO.
PCT/FR00/02978INTERNATIONAL FILING DATE
October 26, 2000PRIORITY DATE CLAIMED
October 28, 1999

TITLE OF INVENTION

Method for Protecting an Electronic System with Modular Exponentiation-Based Cryptography Against Attacks by Physical Analysis

APPLICANT(S) FOR DO/EO/US

Louis GOUBIN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
 - a. ☐ is attached hereto (required only if not communicated by the International Bureau).
 - b. ☒ has been communicated by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
 - a. ☐ is attached hereto.
 - b. ☒ has been previously submitted under 35 U.S.C. 154(d)(4).
- ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
 - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
 - b. ☐ have been communicated by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☐ have not been made and will not be made.
- ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
8. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
9. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
10. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
11. ☐ A copy of the International Search Report (PCT/ISA/210).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☒ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☐ Certificate of Mailing by Express Mail
23. ☐ Other items or information:

Verification of Translator

Formal Drawings (1)

Proposed Drawing Corrections, with 1 red-lined formal drawing

PCT forms: Demande, PCT/IB/301, 308; PCT/RO/101

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.53) 09/869435	INTERNATIONAL APPLICATION NO. PCT/FR00/02978	ATTORNEY'S DOCKET NUMBER T2146-907343
---	---	--

24. The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

- ☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO \$1000.00
- ☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$860.00
- ☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$710.00
- ☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$690.00
- ☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) \$100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =**CALCULATIONS PTO USE ONLY****\$860.00**Surcharge of **\$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).**\$0.00**

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE
Total claims	11 - 20 =	0	x \$18.00
Independent claims	3 - 3 =	0	x \$80.00

\$0.00**\$0.00**Multiple Dependent Claims (check if applicable). ☐**\$0.00****TOTAL OF ABOVE CALCULATIONS =****\$860.00**☐ Applicant claims small entity status. (See 37 CFR 1.27). The fees indicated above are reduced by 1/2.**\$0.00****SUBTOTAL =****\$860.00**Processing fee of **\$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).**\$0.00****TOTAL NATIONAL FEE =****\$860.00**Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) (check if applicable). ☒**\$0.00****TOTAL FEES ENCLOSED =****\$860.00****Amount to be:****refunded**

\$

charged

\$

- a. ☒ A check in the amount of \$860.00 to cover the above fees is enclosed.
- b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1165. A duplicate copy of this sheet is enclosed.
- d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Edward J. Kondracki
 MILES & STOCKBRIDGE P.C.
 Suite 500 - 1751 Pinnacle Drive
 McLean, VA 22102-3833

SIGNATURE

Edward J. Kondracki

NAME

20,604

REGISTRATION NUMBER

June 28, 2001

DATE

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Louis GOUBIN
International
Application No.: PCT/FR00/02978
International
Filing Date: 26 October 2000
U.S. Serial No.: To be Assigned
U.S. Filing Date: June 28, 2001

For: **SECURITY METHOD FOR A CRYPTOGRAPHIC
ELECTRONIC ASSEMBLY BASED ON MODULAR
EXPONENTIATION AGAINST ANALYTICAL ATTACKS**

McLean, Virginia

PRELIMINARY AMENDMENT

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

Please amend the subject application, filed concurrently herewith, as
indicated below:

IN THE TITLE:

Please cancel the title in its entirety and substitute the following new title:

**-- METHOD FOR PROTECTING AN ELECTRONIC SYSTEM WITH MODULAR
EXPONENTIATION-BASED CRYPTOGRAPHY AGAINST ATTACKS
BY PHYSICAL ANALYSIS--**

IN THE SPECIFICATION:

After the title and before the first paragraph on page 1 at line 5, insert the
following heading at the left-hand margin:

--FIELD OF THE INVENTION--;

Page 1, at line 13, insert the following heading at the left-hand margin:

--BACKGROUND OF THE INVENTION--;

Page 7, at line 13, insert the following heading and sentence:

--BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a representation of a smart card.—

Page 7, delete the two paragraphs beginning at line 15 and ending at line 33 in their entirety and insert the following new paragraphs. (Paragraphs showing the changes using underlining and bracketing are included as an attachment at the end of this Preliminary Amendment).

--The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as shown in Fig. 1. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 assigned to the assignee of the present invention. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.--

Page 8, after line 22, insert the following new paragraph:

1. The present invention relates to a method for the detection of a pathogen in a sample, comprising the steps of: (a) providing a sample; (b) amplifying a nucleic acid sequence of the pathogen; (c) detecting the amplified nucleic acid sequence; and (d) identifying the pathogen based on the detected nucleic acid sequence.

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.—

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

Please amend claims 1 – 7, and add new claims 8-11. The claims that follow are a complete set of “clean” claims. The original claims 1-7 marked up to show the changes with underlining and bracketing are included as an attachment to this Preliminary Amendment:

1. (Amended) A method for protecting an electronic system implementing a cryptographic process involving calculation of a modular exponentiation of a quantity (x), said modular exponentiation using a secret exponent (d), comprising breaking down said secret exponent (d) into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret exponent.

2. (Amended) A method according to claim 1, characterized in that said unpredictable values (d_1, d_2, \dots, d_k), are obtained by:

- a) deriving $(k-1)$ values by means of a random generator; and
- b) taking the difference between the secret exponent and the $(k-1)$ values to derive a final value.

3. (Amended) A method according to claim 1, wherein calculation of the modular exponentiation is performed by:

- a) raising the quantity (x) by an exponent comprising said value to obtain a set of results for each of said k values and
- b) calculating a product of the results obtained in step a).

4. (Amended) A method according to claim 1, wherein at least one of said $(k-1)$ values is obtained by means of a random generator and has a length

3 at least equal to 64 bits.

1 5. (Amended) Utilizing the method according to claim 1 in a smart
2 card comprising information processing means.

1 6. (Amended) Utilizing the method according to claim 1 for protecting
2 a cryptographic calculation process using the RSA algorithm.

1 7. (Amended) Utilizing the method according to claim 1 for protecting
2 a cryptographic calculation process using the Rabin algorithm.

Please add the following new claims:

Year	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100
1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	

1 --8. (New claim) A method for protecting an electronic system
 2 implementing a cryptographic process involving calculation of a modular
 3 exponentiation of a quantity (x), said modular exponentiation using a secret
 4 exponent (d), comprising breaking down said secret exponent (d) into a plurality
 5 of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret
 6 exponent; obtaining said unpredictable values (d_1, d_2, \dots, d_k) by deriving ($k-1$)
 7 values by means of a random generator; by raising the quantity (x) by an
 8 exponent comprising a final value and obtaining a set of results for each of said k
 9 values and calculating a product of the set of results and taking the difference
 10 between the secret exponent and the ($k-1$) values to derive the final value.

1 9. (New Claim) A method according to claim 8, wherein at least one of
 2 said ($k-1$) values is obtained by means of a random generator and has a length
 3 at least equal to 64 bits.

1 10. (New Claim) A smart card adapted to protect an electronic system
 2 comprising means for implementing a cryptographic process involving calculation
 3 of a modular exponentiation of a quantity (x), said modular exponentiation using
 4 a secret exponent (d), comprising breaking down said secret exponent (d) into a
 5 plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to
 6 said secret exponent, means for obtaining said unpredictable values ($d_1, d_2, \dots,$
 7 d_k) by a random generator for deriving ($k-1$) values and means for taking the

8 difference between the secret exponent and the $(k-1)$ values to derive a final
9 value.

1 11. (New Claim) A smart card according to claim 10, wherein calculation
2 of the modular exponentiation is performed by:

- 3 a) raising the quantity (x) by an exponent comprising said value to
4 obtain a set of results for each of said k values and
5 b) calculating a product of the results obtained.--

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
220

IN THE ABSTRACT:

Please delete the Abstract at page 11 in its entirety and substitute the following new Abstract.

ABSTRACT
The present invention relates to a method for the detection of a target nucleic acid sequence in a sample. The method comprises the steps of: (a) amplifying the target nucleic acid sequence in the sample using a primer pair; (b) detecting the amplified target nucleic acid sequence using a probe; and (c) determining the presence or absence of the target nucleic acid sequence in the sample based on the detection of the amplified target nucleic acid sequence.

--ABSTRACT

The invention concerns a method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation of a quantity (x), said modular exponentiation using a secret exponent (d), characterized in that said secret exponent is broken down into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret exponent.--

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2

REMARKS

This Preliminary Amendment is filed to insert headings to conform the application to U.S. practice and to correct informalities in the specification, claims and abstract resulting from a literal translation of the French text.

Early action on the merits is earnestly solicited.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: June 28, 2001

By: 

Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

The following are the two paragraphs on page 7 beginning at line 15 and ending at line 33 showing the changes made using underlining and bracketing:

The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as [in the sole figure] shown in Fig. 1. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 [in the name of the Applicant] assigned to the assignee of the present invention. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.

The following are the amended claims marked up to show the changes with underlining and bracketing:

1. (Amended) [Method] A method for protecting an electronic system implementing a cryptographic [calculation] process involving calculation of a modular exponentiation of a quantity (x), said modular exponentiation using a secret exponent (d), [characterized in that] comprising breaking down said secret exponent [is broken down] (d) [in to] into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret exponent.

2. (Amended) [Method] A method according to claim 1, characterized in that said unpredictable values (d_1, d_2, \dots, d_k), are obtained [in the following way] by:

a) deriving ($k-1$) values [are obtained] by means of a random generator; and

b) taking [the final value is obtained from] the difference between the secret exponent and the ($k-1$) values to derive a final value.

3. (Amended) [Method] A method according to claim 1, [characterized in that the] wherein calculation of the modular exponentiation is performed [in the following way] by:

a) [for each of said k values,] raising the quantity (x) [is raised] by an exponent comprising said value [in order] to obtain [a result,] a set of results [thus being obtained] for each of said k values; and

7 b) calculating a product of the results obtained in step a) [is
8 calculated].

1 4. (Amended) [Method] A method according to claim 1,
2 [characterized in that] wherein at least one of said $(k-1)$ values is obtained by
3 means of a random generator and has a length [greater than or] at least equal to
4 64 bits.

1 5. (Amended) [Utilization of] Utilizing the method according to claim 1
2 in a smart card comprising information processing means.

1 6. (Amended) [Utilization of] Utilizing the method according to claim 1
2 [to protect] for protecting a cryptographic calculation process using the RSA
3 algorithm.

1 7. (Amended) [Utilization of] Utilizing the method according to claim 1
2 [to protect] for protecting a cryptographic calculation process using the Rabin
3 algorithm.

1/8/25

09/869435

JC03 Rec'd PC 7/1 28 JUN 2001

**SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC
ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST
ANALYTICAL ATTACKS**

5 The present invention relates to a method for protecting an electronic system implementing an algorithm involving a modular exponentiation, in which the exponent is secret. More precisely, the purpose of the method is to create a version of such an algorithm that is not vulnerable to a certain type of physical attack - called *Differential Power Analysis* or *High-Order Differential Power Analysis*, (abbreviated
10 DPA or HO-DPA) – which tries to obtain information on the secret key from a study of the electric power consumption of the electronic system during the execution of the calculation.

 The cryptographic algorithms considered herein use a secret key to calculate a piece of output information based on a piece of input information; this can involve an
15 encryption, decryption, signature, signature verification, authentication, non-repudiation or key-exchange operation. They are constructed in such a way that a hacker, knowing the inputs and the outputs, cannot in practice deduce any information on the secret key itself.

 We are therefore interested in a class larger than that traditionally designated
20 by the expression *secret key algorithms* or *symmetrical algorithms*. In particular, everything described in the present patent application also applies to so-called *public key* or *asymmetrical algorithms*, which actually include two keys: one public, the other private and not divulged, the latter being the one targeted by the attacks described below.

25 Attacks of the Power Analysis type, developed by Paul Kocher and *Cryptographic Research* (see the document *Introduction to Differential Power Analysis and Related Attacks* by Paul Kocher, Joshua Jaffe, and Benjamin Jun, Cryptography Research, 870 Market St., Suite 1008, San Francisco, CA 94102; HTML edition of the document available at the URL address:
30 <http://www.cryptography.com/dpa/technical/index.html>) start with the observation that in reality the hacker can acquire information other than simply the input and output data during the execution of the calculation, such as for example the power

consumption of the microcontroller or the electromagnetic radiation emitted by the circuit.

Differential power analysis is an attack that makes it possible to obtain information on the secret key contained in the electronic system, by performing a statistical analysis of the power consumption records, performed on a large number of calculations with this same key.

This attack does not require any knowledge of the individual power consumption of each instruction, or on the temporal position of each of these instructions. It applies in the same way assuming that the hacker knows some of the outputs of the algorithm and the corresponding consumption curves. It is based solely on the fundamental hypothesis according to which:

Fundamental hypothesis: There is an intermediate variable appearing during the calculation of the algorithm, such that the knowledge of a few key bits, in practice less than 32 bits, makes it possible to decide whether or not two inputs, respectively two outputs, give the same value for this variable.

The so-called high-order power analysis attacks are a generalization of the DPA attack described above. They can use several different sources of information: in addition to the consumption, they can use measurements of electromagnetic radiation, temperature, etc., performing statistical operations that are more sophisticated than the simple notion of an average, and intermediate variables that are less elementary than a simple bit or a simple byte. Nevertheless, they are based on exactly the same fundamental hypothesis as DPA.

The object of the method that is the subject of the present invention is to eliminate the risk of DPA or HO-DPA attacks on electronic systems with secret or private key cryptography involving modular exponentiation in which the exponent is secret.

Another object of the present invention is consequently to modify the cryptographic calculation process implemented by protected electronic cryptographic systems, in such a way that the aforementioned fundamental hypothesis is not longer verified, i.e. that there is no intermediate variable that depends on the consumption of a sub-system easily accessible by the secret or private key, attacks of the DPA or HO-DPA thus being rendered ineffective.

First example: the RSA algorithm

RSA is the most famous of the asymmetrical cryptographic algorithms. It was developed by Rivest, Shamir and Adleman in 1978. For a more detailed description of this algorithm, it may be useful to refer to the following document:

- R.L. Rivest, A. Shamir, L.M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 21, No. 2, 1978, pp. 120-126,

or to the following documents:

- ISO/IEC 9594-8/ITU-T X.509, *Information Technology – Open systems Interconnection – The Directory: Authentication Framework*;
- ANSI X9.31.1, *American National Standard, Public-Key Cryptography Using Reversible Algorithms for the Financial Services Industry*, 1993;
- PKCS #1, *RSA Encryption Standard*, version 2, 1998, available at the following address: <ftp://ftp.rsa.com/pub/pkcs/doc/pkcs-1v2.doc>.

The RSA algorithm uses a whole number n that is the product of two large prime numbers p and q , and a whole number e , prime with $\text{ppcm}(p-1, q-1)$, and such that $e \cdot \pm 1 \bmod \text{ppcm}(p-1, q-1)$. The whole numbers n and e constitute the public key. The public key calculation uses the function g of $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ defined by $g(x) = x^e \bmod n$. The secret key calculation uses the function $g^{-1}(y) = y^d \bmod n$, where d is the secret exponent (also called the secret or private key) defined by $ed \cdot 1 \bmod \text{ppcm}(p-1, q-1)$.

Attacks of the DPA or HO-DPA type can pose a threat to the standard implementations of the RSA algorithm. In essence, the latter very often use the so called *square and multiply* principle to perform the calculation of $x^d \bmod n$.

This principle consists of writing the breakdown

$$d = b_{m-1} \cdot 2^{m-1} + b_{m-2} \cdot 2^{m-2} + \dots + b_1 \cdot 2^1 + b_0 \cdot 2^0$$

of the secret exponent d in base 2, the performing the calculation in the following way:

1. $z \leftarrow 1$;
- for i running from $m-1$ to 0 perform:
 2. $z \leftarrow z^2 \bmod n$;
 3. if $b_i = 1$ then $z \leftarrow z \times x \bmod n$.

In this calculation, it is clear that among the successive values assumed by the variable z , the prime numbers depend on only a few bits of the secret key d . The fundamental hypothesis that makes the DPA attack possible is therefore fulfilled. It is thus possible to guess, for example, the 10 high-order bits of d by concentrating on the consumption measurements in the part of the algorithm that corresponds to i running from $m-1$ to $m-10$, which makes it possible to find the next ten bits of d , and so on. Eventually, all the bits of the secret exponent d are found.

A first protection method, and its disadvantages

A conventional method (proposed by Ronald Rivest in 1995) for protecting the RSA algorithm against DPA type attacks consists of using a "blinding" principle. This uses the fact that:

$$x^d \bmod n = (x \times r^e)^d \times r^{-1} \bmod n$$

Thus, the calculation of $y = x^d \bmod n$ is broken down into four steps:

- A random generator is used to obtain a value r ;
- We calculate : $u = x \times r^e \bmod n$;
- We calculate : $v = u^d \bmod n$;
- We calculate : $y = v \times r^{-1} \bmod n$.

The disadvantage of this method is that it makes it necessary, for each calculation, to calculate the modular inverse r^{-1} of the random value r , this operation generally being time-consuming (the duration of such a calculation is on the same order as that of a modular exponentiation such as $u^d \bmod n$). Consequently, this new implementation (protected against DPA attacks) of the calculation of $x^d \bmod n$ takes about twice as long as the initial implementation (not protected against DPA attacks). In other words, this protection of RSA against DPA attacks increases the calculation time by approximately **100%** (assuming that the public exponent e is very small, for example $e=3$; if the exponent e is larger, this calculation time is even longer).

A second method: the method of the present invention

According to the invention, a method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation

of a quantity (x), said modular exponentiation using a secret exponent (d), is characterized in that said secret exponent is broken down into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret exponent.

Advantageously, said values (d_1, d_2, \dots, d_k), are obtained in the following way:

- 5 a) ($k-1$) values are obtained by means of a random generator;
- b) the final value is obtained from the difference between the secret exponent and the ($k-1$) values.

Advantageously, the calculation of the modular exponentiation is performed in the following way:

- 10 a) for each of said k values, the quantity (x) is raised by an exponent comprising said value in order to obtain a result, a set of results thus being obtained;
- b) a product of the results obtained in step a) is calculated.

Advantageously, at least one of said ($k-1$) values obtained by means of a random generator has a length greater than or equal to 64 bits.

- 15 Some of the details and advantages of the present invention will emerge from the following description of some preferred but non-limiting embodiments, in reference to the sole attached figure, which represents a smart card.

According to the invention, we use the fact that:

if $d = d_1 + d_2$, then $x^d \bmod n = x^{d_1} \times x^{d_2} \bmod n$

- 20 Thus, the calculation of $y = x^d \bmod n$ is broken down into five steps:

- A random generator is used to obtain a value d_1 ;
- We calculate : $d_2 = d - d_1$;
- We calculate : $u = x^{d_1} \bmod n$;
- We calculate : $v = x^{d_2} \bmod n$;
- 25 • We calculate : $y = u \times v \bmod n$.

- The advantage is that, this way, there is no modular inverse to calculate. In general, the calculation time of a modular exponentiation is proportional to the size of the exponent. Thus, if we let \bullet be the ratio between the size of d_1 and the size of d_2 , it is clear that the total calculation time in this new implementation (protected against
- 30 DPA attacks) is about $(1 + \bullet)$ times the calculation time in the initial implementation (not protected against DPA attacks).

Note that, in order to obtain an unpredictable value d_1 , it necessary for its size to be at least 64 bits.

The method thus described renders attacks of the DPA or HO-DPA type described above ineffective. In essence, in deciding whether or not two inputs (respectively two outputs) of the algorithm give the same value for an intermediate variable appearing during the calculation, it is no longer enough to know the key bits involved. It is also necessary to know the breakdown of the secret key d into k values d_1, d_2, \dots, d_k such that $d=d_1+d_2+\dots+d_k$. Assuming that this breakdown is secret, and that at least one of the k values has a size of at least 64 bits, the hacker cannot predict the values of d_1, \dots, d_k , and therefore the fundamental hypothesis that would make it possible to implement a DPA or HO-DPA type attack, is no longer verified.

Examples:

1. If n has a length of 512 bits, by choosing to take a random value d_1 of 64 bits, we obtain $\bullet = 1/8$, which means that this protection of RSA against DPA attacks increases the calculation time by about **12.5%**.
2. If n has a length of 1024 bits, by choosing to take a random value d_1 of 64 bits, we obtain $\bullet = 1/16$, which means that this protection of RSA against DPA attacks increases the calculation time by about **6.25%**.

Second example: the Rabin algorithm

We will now consider the asymmetrical cryptographic algorithm developed by Rabin in 1979. For a more detailed description of this algorithm, it may be useful to refer to the following document:

- M. O. Rabin, *Digitized Signatures and Public-Key Functions as Intractable as Factorization*, Technical Report LCS/TR-212, M.I.T. Laboratory for Computer Science, 1979.

The Rabin algorithm uses a whole number n that is the product of two large prime numbers p and q , which also verify the following two conditions:

- p is congruent with 3 modulo 8 ;
- q is congruent with 7 modulo 8.

The public key calculation uses the function g of $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ defined by $g(x)=x^2 \bmod n$. The secret key calculation uses the function $g^{-1}(y)=y^d \bmod n$, where d

is the secret exponent (also called the secret or private key) defined by $d=((p-1)(q-1)/4+1)/2$.

The function implemented by the secret key calculation being exactly the same as that used by the RSA algorithm, the same DPA or HO-DPA attacks are applicable and can pose the same threats to the Rabin algorithm.

Protecting the algorithm

Since the function is exactly the same as the one in RSA, the protection method described in the RSA context is applied in the same way in the case of the Rabin algorithm. The increase in the calculation time caused by the application of this method is also the same as in the case of the RSA algorithm.

The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as in the sole figure. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 in the name of the Applicant. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.

In the case of the utilization of such an electronic system, the invention consists in a method for protecting an electronic system comprising information processing means and information storage means, the method implementing a cryptographic calculation process involving a modular exponentiation of a quantity (x) stored in the information storage means, said modular exponentiation using a secret exponent (d) stored in the storage means, characterized in that, by means of said information processing means, said secret exponent read in said information storage means is broken down into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret exponent, said k unpredictable values being stored in the information storage means.

Advantageously, said values (d_1, d_2, \dots, d_k) are obtained in the following way:

a) (k-1) values are obtained by means of a random generator and stored in the information storage means;

b) the final value is obtained from the difference between the secret exponent and the (k-1) values, calculated by means of said information processing means.

Advantageously, the calculation of the modular exponentiation is performed in the following way:

a) for each of said k values, the quantity (x) is raised by an exponent comprising said value in order to obtain a result, a set of results thus being obtained;

b) a product of the results obtained in step a) is calculated.

Advantageously, at least one of said (k-1) values obtained by means of a random generator has a length greater than or equal to 64 bits.

CLAIMS

1 1. Method for protecting an electronic system implementing a cryptographic
2 calculation process involving a modular exponentiation of a quantity (x), said modular
3 exponentiation using a secret exponent (d), characterized in that said secret exponent is
4 broken down in to a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which
5 is equal to said secret exponent.

1 2. Method according to claim 1, characterized in that said values ($d_1, d_2, \dots,$
2 d_k), are obtained in the following way:

- 3 a) ($k-1$) values are obtained by means of a random generator;
4 b) the final value is obtained from the difference between the secret exponent
5 and the ($k-1$) values.

1 3. Method according to claim 1, characterized in that the calculation of the
2 modular exponentiation is performed in the following way:

- 3 a) for each of said k values, the quantity (x) is raised by an exponent
4 comprising said value in order to obtain a result, a set of results thus being obtained;
5 b) a product of the results obtained in step a) is calculated.

1 4. Method according to claim 1, characterized in that at least one of said ($k-$
2 1) values obtained by means of a random generator has a length greater than or equal to
3 64 bits.

1 5. Utilization of the method according to claim 1 in a smart card comprising
2 information processing means.

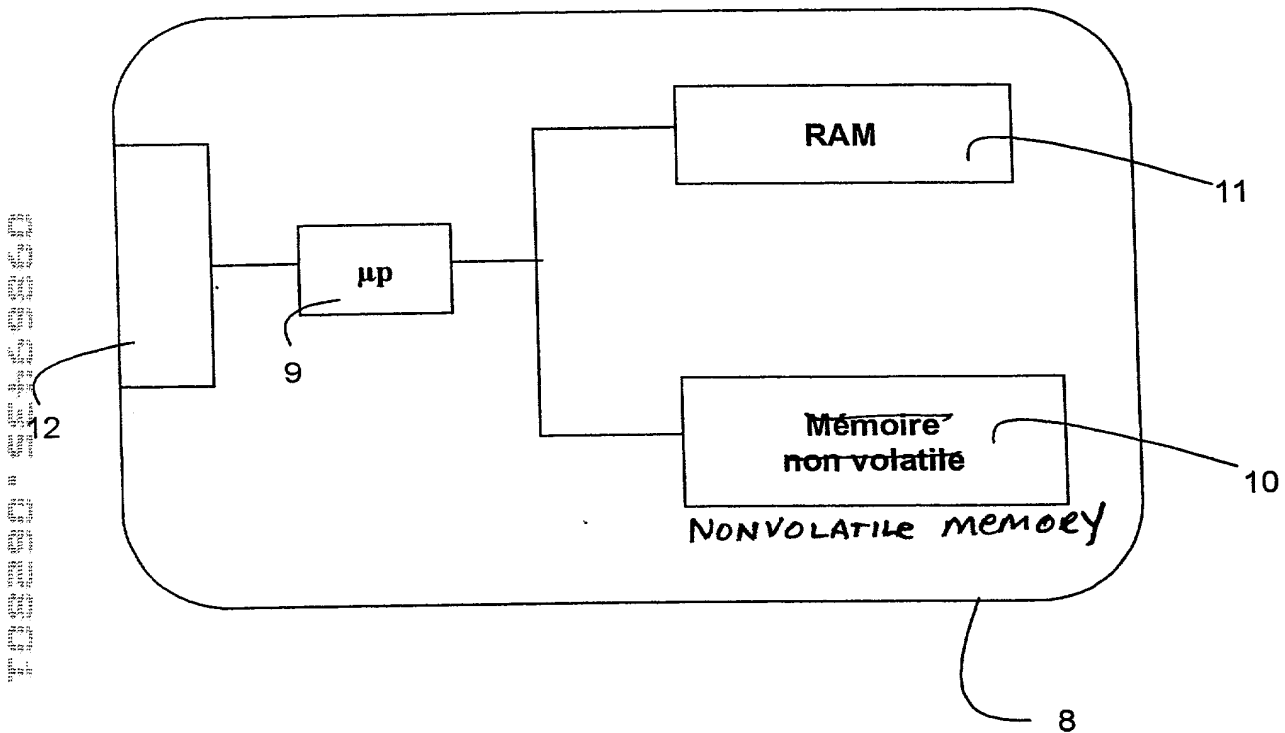
1 6. Utilization of the method according to claim 1 to protect a cryptographic
2 calculation process using the RSA algorithm.

- 1 7. Utilization of the method according to claim 1 to protect a cryptographic
- 2 calculation process using the Rabin algorithm.

ABSTRACT

SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST ANALYTICAL ATTACKS

The invention concerns a method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation of a quantity (x), said modular exponentiation using a secret exponent (d), characterized in that said secret exponent is broken down into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret exponent.



~~FIGURE UNIQUE~~

SOLE FIGURE

US 03857/CORLU Bernard

French Language Declaration

Je revendique par le présent acte le bénéfice de priorité étrangère selon Titre 35, du Code des Etats-Unis, §119 de toute demande de brevet ou d'attestation d'inventeur énumérée ci-après, et j'ai identifié également ci-après toute demande étrangère de brevet ou d'attestation d'inventeur ayant une date de dépôt antérieure à celle de la demande pour laquelle la priorité est revendiquée.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior foreign applications

Demande(s) de brevet antérieure(s) dans un autre pays:

FR 99 13507

France

28 10 1999

(Number)
(Numéro)(Country)
(Pays)(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)

Priority claimed

Droit de priorité
revendiqué☒
Yes
Oui☐
No
Non(Number)
(Numéro)(Country)
(Pays)(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)☐
Yes
Oui☐
No
Non(Number)
(Numéro)(Country)
(Pays)(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)☐
Yes
Oui☐
No
Non

Je revendique par le présent acte, le bénéfice selon Titre 35 du Code des Etats-Unis, §120 de toute(s) demande(s) américaine(s) énumérée(s) ci-après et, dans la mesure où le sujet de chacune des revendications de cette demande n'est pas divulgué dans la demande américaine antérieure, de la façon définie par le premier paragraphe de l'article 35 du Code des Etats-Unis, §112, je reconnais le devoir de divulguer l'information pertinente selon Titre 37 du Code des Règlements Fédéraux, §1.56(a), toute information qui se présente entre la date de dépôt de la demande antérieure et la date de dépôt de la demande, soit nationale, soit internationale PCT.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PCT/FR 00/02978

26/10/00

(Application Serial No.)
(No. de Demande)(Filing Date)
(Date de Dépôt)

PENDING

(Elat)
(brevetée, pendante,
abandonnée)(Status)
(patented, pending,
abandoned)(Application Serial No.)
(No. de Demande)(Filing Date)
(Date de Dépôt)(Elat)
(brevetée, pendante,
abandonnée)(Status)
(patented, pending,
abandoned)

Je déclare par le présent acte que toutes mes déclarations, à ma connaissance, sont vraies et que toutes les déclarations faites à partir de renseignements ou de suppositions, sont tenues pour être vraies; de plus, toutes ces déclarations ont été faites en sachant que de fausses déclarations volontaires ou autres actes de même nature sont sanctionnées par une amende ou un emprisonnement, ou les deux, selon la Section 1001, du Titre 18 de Code des Etats-Unis et que de telles déclarations délibérément fausses peuvent compromettre la validité de la demande ou du brevet délivré.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

US 03857/CORLU Bernard

French Language Declaration

POUVOIR: En tant qu'inventeur, je désigne l'(les) avocat(s) et/ou l'(les) agent(s) suivant(s) pour poursuivre la procédure de cette demande et traiter toute affaire la concernant auprès du Bureau des Brevets et de Marques:

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

Adresser toute correspondance à:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Send Correspondence to:

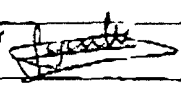
Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Adresser toute communication téléphonique à:
(Nom) (Numéro de téléphone)

Edward J. Kondracki, Esq.
(703) 998-3302

Direct Telephone Calls to: (name and telephone number)

Edward J. Kondracki, Esq.
(703) 998-3302

Nom complet du seul ou premier inventeur		Full name of sole or first inventor	
GOUBIN Louis			
Signature de l'inventeur	Date	Inventor's signature	Date
	21/06/01		
Domicile		Residence	
3 rue Brown-Séguard 75015 PARIS FRANCE JRX			
Nationalité		Citizenship	
Française			
Adresse Postale		Post Office Address	
3 rue Brown-Séguard 75015 PARIS FRANCE			
Nom complet du second co-inventeur, le cas échéant		Full name of second joint inventor, if any	
Signature de l'inventeur	Date	Second inventor's signature	Date
Domicile		Residence	
Nationalité		Citizenship	
Adresse Postale		Post Office Address	

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)

Declaration and Power of Attorney For Patent Application

Declaration Pour Demandes de Brevets Avec Pouvoirs

French Language Declaration

En tant qu'inventeur nommé ci-après, Je déclare par le présent acte que:

Mon nom, mon domicile, mon adresse postale, ma nationalité sont ceux qui figurent ci-après,

Je déclare que je crois être l'inventeur original, premier et unique (si un seul nom figure sur le présent acte) ou un des co-inventeurs, originaux et premiers (si plusieurs noms figurent sur le présent acte) du sujet revendiqué et pour lequel un brevet est demandé sur la base de l'invention intitulée:

Procédé de sécurisation d'un ensemble électronique de cryptographie à base d'exponentiation modulaire contre les attaques par analyse physique.

(dont la description

(cocher la case correspondante)

☒ est annexée au présent acte.

☐ a été déposée _____

Numéro de série de la demande _____

et modifiée le _____ (si approprié)

Je déclare par le présent acte avoir examiné et compris le contenu de la description identifiée ci-dessus, revendications y compris, et le cas échéant telle que modifiée par l'amendement cité plus haut

Je reconnais le devoir de divulguer l'information qui est en rapport avec l'examen de cette demande selon Titre 37 du Code des Règlements Fédéraux §1.56(a).

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

the specification of which

(check one)

☐ is attached hereto.

☐ was filed on _____ as

Application Serial No. _____

and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

T2146-907343-US 3857/BC(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Louis GOUBIN

International
Application No.: PCT/FR00/02978

International
Filing Date: 26 October 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: June 28, 2001

For: **METHOD FOR PROTECTING AN ELECTRONIC SYSTEM
WITH MODULAR EXPONENTIATION-BASED
CRYPTOGRAPHY AGAINST ATTACKS BY PHYSICAL
ANALYSIS**

McLean, Virginia

CHANGE OF ADDRESS

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Effective immediately, please note our new correspondence address and
telephone/fax numbers as follows:

Miles & Stockbridge P.C.
1751 Pinnacle Drive
Suite 500
McLean, VA 22102-3833
Telephone: 703-903-9000
Fax: 703-610-8686

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

By:

Edward J. Kondracki
Edward J. Kondracki
Registration No. 20,604

Date: June 28, 2001

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686